Résumé : Fuite massive de données : 16 milliards d'identifiants e-mail/mot de passe sont en circulation. Changez vos mots de passe, activez la 2FA, et vérifiez vos comptes.

Source : https://cybernews.com/security/billions-credentials-exposed-infostealers-data-leak/
Cet article à été coécrit avec ChatGPT

🌐 Fuite massive de données : 16 milliards d'identifiants en circulation

Une nouvelle alerte cybersécurité vient de tomber : selon une enquête de Cybernews.com, plus de 16 milliards de combinaisons e-mail/mot de passe circulent librement sur des forums de hackers et des services en ligne douteux.

📥 D'où ça vient ?

Ce n'est pas une seule grosse fuite, mais plutôt les années de vols de données, surtout via des infostealers : des malwares qui s'installent discrètement sur les ordis et aspirent tout ce qu'ils trouvent (logins, cookies, données de navigateur…).
Les infos viennent de dizaines de fichiers compilés, avec parfois des doublons, mais aussi des identifiants valides récents.

🧨 Pourquoi c'est un gros risque ?

- Les pirates peuvent faire du credential stuffing : tester automatiquement ces identifiants sur plein de sites
- Certains fichiers contiennent aussi des cookies de session ou des tokens, donc parfois pas besoin du mot de passe pour accéder au compte
- Il y a des accès à tout : mails, réseaux sociaux, outils pros, services cloud, etc.
- Même si tu penses que tu n'as rien d'important, un accès à ton mail suffit à réinitialiser plein de comptes

✅ Que faire maintenant ?

Voici des trucs simples à faire :

1. Change tes mots de passe, surtout sur les comptes sensibles (mail, banque, réseaux sociaux)
2. Utilise un mot de passe différent par compte (avec un gestionnaire c'est plus simple)
3. Active l'authentification à deux facteurs (2FA) partout où c'est possible
4. Va vérifier si tes mails ont fuité sur haveibeenpwned.com (mais je suis pas sur qu'ils ont cette base de donnée, à vérifier. Sinon j'ai vu que Cybernews aussi avait son outil allez y faire un tour https://cybernews.com/password-leak-check/)

5. Fait une analyse antivirus sur ton PC (Windows + R, écrivez MRT sous windows)
6. Attention aux mails bizarres ou trop beaux pour être vrais (genre "Prolongez votre Netflix alors que t'as pas Netflix, ou gagné un truc sans participer à rien)